



Reporting and Notification to Individuals



***Presented by
Samuel P. Jenkins***

***Director, Defense Privacy and
Civil Liberties Office***

**2010 DoD FOIA/PA Conference
Germany - April 28, 2010**



Reporting and Notification: Reporting Timeframe

Reporting Requirements Timeframe

- **Annual** - Privacy Section D of Federal Information Security Management Act (FISMA) Report (Due August 17, 2009)
- **Annual** - SSN Reduction Review Report (Due August 17, 2009)
- **Quarterly** - Training/SORN and Section 803 Report, due the 15th of the month following the end of quarter. If the 15th falls on a weekend, submit by COB the next work day.)
- **Episodic** - Breach Report. Due on **1-24-48** hours timeline.



Compliance Reporting Authority

Chapter Eight of the DoD 5400.11-R, “Department of Defense Privacy Program Regulation”, May 14, 2007.

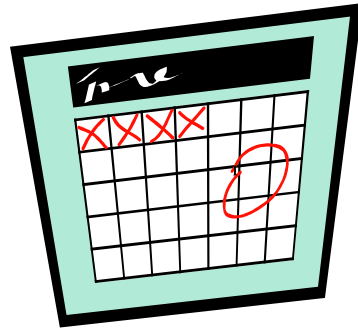
C8.1 The Defense Privacy Office shall establish requirements for DoD Privacy Reports and the DoD Components shall be required to provide data.

**C8.2 The suspenses for submission of all reports shall be
established by the Defense Privacy Office.**



Reporting Notification: Annual Reports

The “Annuals”





Reporting and Notification: Annual Reports

Authorities: Federal Information Security Management Act (FISMA), E-Government Act of 2002, Section 208 (Public Law 107-347) and;

- ***DPO Memorandum, DoD Privacy Reporting Guidance for the Federal Information Security Management Act (FISMA), July 8, 2009***
- **Purpose: To provide a framework for enhancing the effectiveness of information security in the federal government. This means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to ensure integrity, confidentiality and availability.**
- **Due Date: August 17, 2009**



Federal Information Security Management Act (FISMA) 2009 Reporting Guidance

- **July 8, 2009 DPO Director Memo/templates/supplemental guidance Issue**
 - **Reporting period July 1, 2008 - June 30, 2009.**
- **Outlined anticipated response requirements related to SAOP reporting requirements:**
 - **Privacy Act Component SORNs and training**
 - **Agency privacy procedures and practices**
 - **Internal oversight mechanism for privacy**
- **Complete Section D, reporting Template for SAOP found in attachment 2 of memo by August 17, 2009**



FISMA

Reporting and Notification: Annual Reports (con't)

Microsoft Excel - m08-21_section_d_saop_template.xls

UNCLASSIFIED//FOUO

copy screen

File Edit View Insert Format Tools Data Window Help Adobe PDF

100% Arial 11

Reply with Changes... End Review...

D2

Section D - Senior Agency Official for Privacy (SAOP): Questions 7 - 11

Agency Name: [Redacted]

7. Written Privacy Complaints

In the table provided, indicate the number of written complaints for each type of privacy issue allegation received by the SAOP, in addition to the number of complaints for each type each type of complaint. Written complaints do not include Freedom of Information Act requests or Privacy Act access requests:

Type	Number of complaints
a. Process and Procedural -- consent, collection, and appropriate notice)	
b. Redress -- non-Privacy Act inquiries seeking resolution of difficulties or concerns about privacy matters	
c. Operational -- inquiries regarding Privacy Act matters not including Privacy Act requests for access/ and/or correction	
d. Referrals -- complaints referred to another agency with jurisdiction	

= Data Entry Cells

8. Policy Compliance Review

8.a. Does the agency have current documentation demonstrating review of compliance with information privacy laws, regulations, and policies? Yes or No.

8.b. Can the agency provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews? Yes or No.

8.c. Does the agency use technologies that enable continuous auditing of compliance with stated privacy policies and practices? Yes or No.

8.d. Does the agency coordinate with the agency's Inspector General on privacy program oversight? Yes or No.

9. Information About Advice Provided by the SAOP

Please state "Yes" or "No" to indicate if the SAOP has provided formal written advice in each of the listed categories, and briefly describe the advice in the space provided. For descriptions of training, please provide the number of employees (or contractors) who participated in the training.

9.a. Agency policies, orders, directives, or guidance governing agency handling of personally identifiable information

briefly describe the advice: [Redacted]

9.b. Written Agreements (either Interagency or with Non-Federal Entities)

briefly describe the advice: [Redacted]

9.c. Reviews or feedback outside of the SORN and PIA process (e.g. formal written advice in the context of a hydrology or programmatic planning)

Section D - SAOP #1 Section D - SAOP #2-6 Section D - SAOP #7-11 Control /

Ready

It's not as bad as
it looks,
really.





Reporting and Notification: Annual Reports (con't)

Authorities: Directive-Type Memorandum (DTM) 07-015-USD(P&R), March 28, 2008 - DoD Social Security Number (SSN) Reduction Plan;

- **OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2, 2007, Attachment 1, B.2., Reduce the Use of Social Security Numbers.**
- **Purpose: It is DoD policy to reduce or eliminate the use of SSN wherever possible.**
 - ***One way to accomplish this effort is to review SSN usage on new and existing Component-wide forms.***
- **Due Date: August 17, 2009 - At the same time of FISMA Report.**



Thinking Through the Challenge

- **During the SSN reduction evaluation phase, users should be looking to improve security and protection for SSNs they have in their systems.**
- **Documentation of completed reviews should show that users have really looked for alternatives to use of SSNs.**
- **It is unacceptable to simply say it can't be done.**



Reporting and Notification: Annual Reports (con't)

It's Not All About Social Security Numbers (SSNs)

- **SSNs are high profile, but not the only concerns.**
- **Have to think about all Personally Identifiable Information and collect only what is REALLY needed!**
- **This is about protecting ourselves, the organization and reducing the liability for both.**



Reporting and Notification: Annual Reports (con't)

SSN Forms Review Memo (U) - Message (Plain Text) UNCLASSIFIED//FOUO

SSN Forms Review Reporting Template (3).pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

Create PDF Combine Files Export Secure Sign Forms Review & Comment

2 / 2 75% Find

ATTACHMENT

Social Security Number (SSN) Forms Review Report

DoD Component:

DoD Component Forms Manager (Responsible Component Forms Management Officer who can answer questions regarding the submitted report.)

Name: Title:

Phone Number: Email Address:

Mailing Address:

FOR FORMS EXISTING AS OF JUNE 30, 2008

Total Number of Forms in Database	Number of Forms Reviewed	Number of Forms Containing SSNs	Number of Forms Where Justifications Were Questioned	Number of SSN Justifications Accepted	Number of SSN Justifications Rejected

Additional Instructions:

List form numbers and titles for all forms where SSNs were not allowed.

List form numbers and titles for all forms where SSNs were masked or truncated.

FOR FORMS SUBMITTED FOR APPROVAL JULY 1, 2008 – JUNE 30, 2009

Number of Forms Reviewed	Number of Forms Requesting SSNs	Number of SSN Justifications Accepted	Number of SSN Justifications Rejected

Additional Instructions:

List form numbers and titles for all forms where SSNs were not allowed.

List form numbers and titles for all forms where SSNs were masked or truncated.

Start | Address | http://www.whs.mil/ | 8:12 AM Thursday



Reporting and Notification: Quarterly Reports

THE “QUARTERLY’S”





Reporting and Notification: Quarterly Reports

Authorities: OMB Circular A-130, Appendix I, “Management of Federal Information Resources,” November 28, 2000, Appendix I, para 3.a., (8) defines SORN responsibility reviews; and

- DoD 5400.11, DoD Privacy Program, May 8, 2007;
 - DoD 5400.11-R Department of Defense Privacy Program, May 27, 2007;
 - The Federal Information Security Management Act of 2002;
 - DA&M Memorandum, Appointment of a Senior Official for Privacy and Issuance of Revised Program Compliance Reporting Requirements, Feb 7, 2008.
-
- **Purpose: Status of the DoD Components’ review and coordination of the Privacy Act systems of records procedure.**
 - **Due Date: Quarterly - To DPO by the 15th of the month following the end of quarter. If the 15th falls on a weekend, submit by COB the next working day.**



Reporting and Notification: Quarterly Reports (con't)

Microsoft Excel - SORNs-Training-803 Reports Template-version 11 (version 1) UNCLASSIFIED//FOUO

File Edit View Insert Format Tools Data Window Help Adobe PDF

100%

Arial 10

SORNs

(Select One)

3rd Quarter (Apr-Jun 09)

(REPORTS ARE DUE TO DPO BY THE 15TH OF THE MONTH FOLLOWING THE END OF QUARTER!)

CORDS NOTICES REVIEW

SORN NAME	Accurately Describes System Records (Select One)	Accurately Describes NARA's Retention & Disposal (Select One)	Appropriate Routine Use Disclosures (Select One)	Is Exemption Still Required (Select One)	Federal Register Page Number & Date	Comments
NEW REPORT:						
Training Category	Delivery Method	Number Trained (This Quarter)	Number Trained (Yr to Date)	Appx. Number Assigned to Organization	Comments	
Orientation of Newly Reported Personnel	Classroom Brief					
Specialized Training	Poster/Handouts User Guides Distributed					
Management Training	Computer-Assisted or One-on-One as Needed					
SORNs Training	Computer-Assisted & Classroom Brief					
Annual Refresher						
Other						

SORNs-Training Report / 803 Report

Ready



Reporting and Notification: Quarterly Reports (con't)

Authorities: Special job requirements. Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," November 28, 2000, Appendix I, para 3.a., (6) defines training responsibility reviews.

- Part II, Training, of the June 5, 2009 *DoD Memorandum, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*

- Outlined in Chapter 7 of the DoD 5400.11-R, "Department of Defense Privacy Program Regulation", May 14, 2007.

- Purpose: Ensure that all Agency personnel are familiar with the requirements of the Privacy Act, with the agency's implementing regulations, and with any special requirements of their specific jobs.**
- Due Date: Quarterly - To DPO by the 15th of the month following the end of quarter. If the 15th falls on a weekend, submit by COB the next work day.**



Reporting and Notification: Quarterly Reports (con't)

Microsoft Excel - SORNs-Training-803 Reports Template-version 11 (version 1) UNCLASSIFIED//FOUO

File Edit View Insert Format Tools Data Window Help Adobe PDF

100%

Reply with Changes... End Review...

Arial 10 B I U

14

	C	D	E	F	G	H	I	J	K
1	(Select One)						RCS: DA&M(AR) 1379		
2									
3	3rd Quarter (Apr-Jun 09)								
4	(REPORTS ARE DUE TO DPC BY THE 15TH OF THE MONTH FOLLOWING THE END OF QUARTER!)								
5									
6	CORDS NOTICES REVIEW								
7									
8	SORN NAME	Accurately Describes System Records (Select One)	Accurately Describes MARA's Retention & Disposal (Select One)	Appropriate Routine Use Disclosures (Select One)	Is Exemption Still Required (Select One)	Federal Register Page Number & Date	Comments		
9									
10									
11									
12									
13									
14									
15	NEW REPORT:								
16	Training Category	Delivery Method	Number Trained (This Quarter)	Number Trained (Yr to Date)	Appx. Number Assigned to Organization	Comments			
17									
18	Orientation of Newly Reported Personnel	Classroom Brief							
19	Specialized Training	Poster/Handouts User Guides Distributed							
20	Management Training	Computer-Assisted or One-on-One as Needed							
21	SORNs Training	Computer-Assisted & Classroom Brief							
22	Annual Refresher								
23	Other								
24									

SORNs-Training Report / 803 Report /

Draw AutoShapes

Ready



Reporting and Notification: Quarterly Reports (con't)

**Authority: National Security Intelligence
Reform Act (Public Law 110-53, Section 803)**

- **Purpose: To periodically review agency's implementation procedures, policies, and guidelines relating to efforts to protect the Nation against terrorism.**
- **Due Date: Quarterly - To DPO by the 15th of the month following the end of quarter. If the 15th falls on a weekend, submit by COB the next work day.**



Reporting and Notification: Quarterly Reports

The “Section 803 Report”

- **Report shall include information on the discharge of each of the functions of the officer concerned, including:**
 - **Information on the number and types of reviews undertaken;**
 - **The type of advice provided and the response given to such advice;**
 - **The number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and**
 - **A summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.**



Reporting and Notification: Quarterly Reports (con't)

Microsoft Excel - SORNs-Training-803 Reports Template-version 11 (version 1) UNCLASSIFIED//FOUO

File Edit View Insert Format Tools Data Window Help Adobe PDF

100%

Reply with Changes... End Review...

Arial 10 B I U

E34

Component

DPO

Privacy Act Statements(PAS)
Computer Matching Agreements

TOPICS OF ADVICE & RESPONSES GIVEN:

Topics of Advice	Responses Given					
	Procedure Revision	New Guidance Issued	Training Conducted	Developed Policy/Program Interpretation	Memorandum	Briefing
Privacy Act Program Overview/Principles/Policy						
Privacy Act Systems of Records Notices(SORNs)						
Privacy Impact Assessment (PIA)						
SSN and PII Reduction Actions						
PII Breach Management Reporting/Notification						
Privacy Reports						
Privacy Act Violations						

PRIVACY COMPLAINTS AND DISPOSITIONS

Type/Nature of Complaint or Alleged Violation	Number of Complaints	Disposition of Complaint		
		Responsive Action Taken	No Action Required	Pending
1. Processes & Procedures				
2. Redress				

803 Report

Start | Address http://www.whs.mil/ | 8:18 AM Thursday



Reporting and Notification: Breach Management and Reporting

The “Episodic” Reports





Reporting and Notification: Breach Management and Reporting

- **Lost, Stolen or Compromised Information.** Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information when persons other than authorized users gain access or potential access to such information for an other than authorized purposes when one or more individuals will be adversely affected. Such incidents also are known as breaches. *DOD 5400.11-R, DL.1.10*



High Risk Areas

- **Laptop Security**
 - **Physical security**
 - **Software safeguards**
- **Misdirected emails**



High Risk Areas (cont'd)

- **Paper Records**
 - **Retirement and disposal**
 - **Chain of custody**
- **Shared Workspaces**



- **Personal information/Personally Identifiable Information**
- **Actual or possible event**
- **Loss of control**
- **Unauthorized disclosure, or unauthorized access**
- **Adverse affect**



Reporting and Notification: Phase 2: Report the Breach

Breach Reporting Requirement Upon Awareness of Actual or Suspected Breach

WITHIN	REPORT TO
1 Hour	United States Computer Emergency Readiness Team (US- CERT)
24 Hours	Senior Component Privacy Official
48 Hours	Defense Privacy and Civil Liberties Office (DPCLO)



Report ALL breaches

- **US-CERT requires the reporting of only computer incidents**
- **OMB M-06-19 expanded the US-CERT reporting requirement to include “all” incidents**
- **US-CERT <http://www.us-cert.gov/>**
- **US-CERT Incident Reporting <https://forms.us-cert.gov/report/>**



“All” incidents, includes

- Suspected and confirmed incidents**
- Incidents involving PII in electronic or physical form**

**Requirement implemented by CIO
Memo, “DoD Guidance on
Protecting Personally Identifiable
Information”, August 18, 2006**



Reporting and Notification: Phase 3: Investigate the Breach

Get the facts

- **When was the PII compromised?**
- **Whose PII?**
- **What PII?**
- **Where was the PII?**
- **How was the PII compromised?**



Reporting and Notification: Phase 3: Investigate the Breach

Administrative safeguards

- Privacy Act and IA training records**
- Data backup schedules**
- Periodic security audits**
- Access permission policies**
- Data destruction policies**
- Contract and MOU language**



Reporting and Notification: Phase 3: Investigate the Breach

Technical safeguards

- **Encryption software**
- **PKI Certificates/CAC enabled**
- **Password protection**
- **Firewall**
- **Biometrics**



Reporting and Notification: Phase 3: Investigate the Breach

Physical safeguards

- **Security guards**
- **Locks (door, laptop)**
- **Closed circuit TV**
- **Safes**

Reporting and Notification: Phase 4: Assess the Breach



Level of Risk

Degree of Impact

Individual notification within 10 working days

3rd Party
Notification

Credit
Monitoring



- **Were your initial considerations and understanding of the breach accurate?**
- **If lost hardware was involved, was it recovered?**
- **In the end, how many individuals were impacted?**
- **What were the mitigating actions taken in the circumstance of the breach?**



- **Trust ... but verify**
- **Contain the breach**
- **Revise policy; adjust SOPs**
- **Escalate issue to senior management, if necessary**
- **Recognize the human factor**
- **The next realm of breaches**
 - **Social networking sites**
 - **Cloud computing**



Reporting and Notification: Phase 6: Act

DoD Policy and Guidance

OMB Memoranda

CIO Memorandum “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media”, July 3, 2007

OMB M-06-15
OMB M-06-16

CIO Memorandum “DoD Guidance on Protecting Personally Identifiable Information”, August 18, 2006

OMB M-06-15
OMB M-06-16
OMB M-06-19
OMB M-07-16

DoD 5400.11-R “DoD Privacy Program” May 14, 2007

OMB M-05-08
OMB M-06-15
OMB M-06-19
OMB Memo, Sep 20, 2006
OMB M-07-16

DAM Memorandum “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”, June 5, 2009

OMB M-06-15
OMB Memo, Sep 20, 2006
OMB M-07-16

DTM 07-015 “DoD Social Security Number Reduction Plan”, May 2009

OMB M-07-16



Where does it all go?

- **FISMA Report** - DoD CIO, IG and DPO inputs are drafted into one DoD Report submitted to Congress.
- **SSN Reduction Report** -Input into the annual FISMA Report submitted to Congress.
- **Breach Report** - Information provided to DoD Senior Privacy Official weekly. May share breach report with the Secretary of Defense.
- **SORNs/Training Report** - To OMB Director (DoD IG Interest item).
- **Section 803 Report** - To eight different committees of Congress. Public posting.



Reporting and Notification: Notification

Notification When Information is Lost, Stolen, or Compromised



Notification When Information is Lost, Stolen, or Compromised

- If records containing personal information are lost, stolen, or compromised. The personal impact on the affected individual may be severe if the records are misused.
- To assist the individual, the Component shall promptly notify the individual of any loss, theft, or compromise.



1. Notification shall be made whenever a breach involves:
 - A service member, civilian employee, military retiree, family member, contractor, other persons affiliated with the Component (e.g. volunteers), and/or any other member of the public on whom information is maintained.
2. Notification shall be made ASAP, but not later than 10 working days after the breach is discovered and the identities of the affected individuals ascertained.



3. When the information is maintained by a contractor on behalf of a Component, they shall notify the Component immediately after a breach is discovered.
4. If the Component cannot notify within 10 working days, the Component shall inform the Deputy Secretary of Defense of the reasons why.



5. Notice to the individual, at a minimum, shall include:

- What data was involved.
- Facts and circumstances surrounding the breach.
- What protective actions the Component is taking or the individual can take.



Reporting and Notification: Notification

Sample Notification Letter

Dear Mr. John Miller:

On January 1, 2006, a DoD laptop computer was stolen from the parked car of a DoD employee in Washington, D.C. after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program. The compromised information is the name, social security number, residential address, date of birth, office and home email address, office, and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities, who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.



Reporting and Notification: Notification

Sample Notification Letter (cont'd)

You should be guided by the actions recommended by the Federal Trade Commission (FTC) at its Web site at http://www.consumer.gov/idtheft/con_steps.htm. The FTC urges that you immediately place an initial fraud alert on your credit file. The Fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The Department of Defense takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you.

Should you have any questions, please call _____.

Sincerely,

Signature Block
(Directorate level or higher)



“Business as usual is not acceptable”



